

## REMARKS

### Double Patenting

The examiner rejected Claims 1-33 on the ground of non-statutory obviousness-type double patenting as being unpatentable over amended claims 1-24 of co-pending application 10/701,154.

The examiner argues that:

...in the instant case, all elements of claims 1-33 correspond to the claims of 1-24 of the copending application, except in the instant claims the elements "determining whether that one host attempting to gain access has accessed the other host accessed previously; and if that one host has not accessed the other host previously" referred in the copending claims as "to collect connection information to identify host connection pairs from packets that are sent between nodes on a network". Copending claims recite, "determine at least in part from connection patterns derived from the connection table occurrences of network events that indicate potential network intrusion" which encompasses the instant application claims "determining other anomalies includes determining whether previous connection patterns of the hosts indicate that the host are in roles that are not normal for the hosts" and "anomalies includes determining if several short connections occur over a short time period by examining connection behavior between two hosts based on connection pattern data retrieved from the connection table". Thus copending application claims anticipates the instant claims.

Claim 1 of the instant application (as currently amended) is:

1. A computer implemented method comprising:  
retrieving connection pairs from a connection table for a host that is attempting to gain access to another host in a networked computer system;  
determining whether that one host attempting to gain access has accessed the other host previously; and if that one host has not accessed the other host previously,  
determining if other anomalies in the connection patterns of each host exist to establish an event severity level indicating a likelihood that the host attempting to access another host is attempting an unauthorized access.

Claim 1 of the '154 application is:

1. A system, comprising:
  - a plurality of collector devices that are disposed to collect connection information to identify host connection pairs from packets that are sent between nodes on a network; and
  - an aggregator device that receives the connection information from the plurality of collector devices, and which produces a connection table that maps each node on the network to a record that stores information about packet traffic to or from the node, with the aggregator device further comprising:
    - a process executed on the aggregator device to detect anomalies in connection patterns; and
    - a process executed on the aggregator device to aggregate detected anomalies into the network events with the anomalies that are detected including denial of service attack anomalies and scanning attack anomalies.

Claim 1 of the instant application is directed to a technique that uses connection pattern information and existence of other anomalies to detect unauthorized access. In contrast, claim 1 of the co-pending application '154 is directed to a technique that aggregates detected anomalies into network events that can correspond to denial of service attack and scanning attack anomalies. These claims are directed to patentably distinct subject matter with one set of claims neither being anticipated by or obvious over the other.

Therefore, the rejection is improper and should be removed.

The examiner rejected Claims 1-33 on the ground of non-statutory obviousness-type double patenting as being unpatentable over amended claims 1-22 of co-pending application 10/701,353. The examiner stated:

Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant case, all elements of claims 1-33 correspond to the claims of 1-22 of the copending application, except in the instant claims the elements "determining whether that one host attempting to gain access has accessed the other host accessed previously; and if that one host has not accessed the other host previously" referred in the copending claims as "detecting scans emanating from hosts; analyzing records of scans to determine receivers of a scan and to determine which of those receivers of scans later became sources for a subsequent scan". Copending claims recite, "analyzing scan anomalies for the sets of the hosts scanned" and "executing a scan detection process to determine hosts that were targets of scans" which encompasses the instant application claims

**"determining other anomalies includes determining whether previous connection patterns of the hosts indicate that the host are in roles that are not normal for the hosts". Thus copending application claims anticipates the instant claims.**

Claim 1 of the instant application (as currently amended) is reproduced above.

Claim 1 of the '353 application is:

1. A method comprising:  
detecting scans emanating from hosts;  
analyzing records of scans to determine receivers of a scan and  
to determine which of those receivers of scans later became  
sources for a subsequent scan; and  
reconstructing the path by which a worm spread based on the  
analyzed records; and  
sending notification of the reconstructed path to a console.

Claim 1 of the instant application is directed to a technique that uses connection pattern information and existence of other anomalies to detect unauthorized access, as stated above. In contrast, claim 1 of the co-pending application '353 is directed to the detection of a worm attack by reconstructing the path by which a worm spreads based on analyzed scan records. These claims are directed to patentably distinct subject matter and therefore neither of the sets of claims are anticipated by or obvious over the other.

The examiner rejected Claims 1-33 on the ground of non-statutory obviousness-type double patenting as being unpatentable over amended claims 1-36 of co-pending application 10/701,356. The examiner stated:

**Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant case, all elements of claims 1-33 correspond to the claims of 1-36 of the copending application, except in the instant claims the elements "retrieving connection pairs from a connection table for a host that is attempting to gain access to another host" referred in the copending claims as "a memory storing a connection table that maps each node of network to a host object, the connection table stores information about traffic to or from the node". Copending claims recite, "a process to aggregate anomalies into the network events according to connection patterns" which encompasses the instant application claims "determining other anomalies includes using heuristics provide an indication to an operator that elevates severity of a possible unauthorized access event". Thus copending application claims anticipates the instant claims.**

Claim 1 of the instant application (as currently amended) is reproduced above.

Claim 1 of the '356 application is:

1. A device, comprising:
  - a processor;
  - a memory storing:
    - a connection table that maps each node of a network to a host object, the connection table stores information about traffic to or from the node; and
    - an process to detect anomalies based on information in the connection table and to aggregate the anomalies into the network events according to connection patterns.

Claim 1 of the instant application is directed to a technique that uses connection pattern information and existence of other anomalies to detect unauthorized access, as stated above. In contrast, claim 1 of the co-pending application '356 is directed to detecting anomalies based on information in the connection table and aggregating the anomalies into the network events according to connection patterns. These claims are directed to patentably distinct subject matter and therefore neither of the sets of claims are anticipated by or obvious over the other.

The examiner rejected Claims 1-33 on the ground of non-statutory obviousness-type double patenting as being unpatentable over amended claims 1-21 of copending application 10/701,376. The examiner stated:

Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant case, all elements of claims 1-33 correspond to the claims of 1-21 of the copending application, except in the instant claims the elements "determining whether that one host attempting to gain access has accessed the other host accessed previously; and if that one host has not accessed the other host previously" referred in the copending claims as "determining whether a variance in the parameter for the found anomaly exceeds a threshold; and if the variance exceeds that threshold collecting those found anomalies that exceed the threshold into at least one operationally relevant event indicating a detected event in the network". Copending claims recite, "detecting conditions in a network ... further comprising determining event severity" which encompasses the instant application claims "determining if other anomalies in the connection patterns of each host exist to establish an event severity level indicating a likelihood that the host attempting to access another host is attempting an unauthorized access". Thus copending application claims anticipates the instant claims.

Claim 1 of the instant application (as currently amended) is reproduced above.

Claim 1 of the '376 application is:

1. A computer implemented method for detecting conditions in a network, comprising:
  - finding anomalies, which are low-level differences in network operation relative to some comparison period, by:
    - producing a moving average of a parameter associated with network packet flows;
    - determining whether a variance in the parameter exceeds a threshold; and if the variance exceeds the threshold to indicate an anomaly,
    - collecting the anomaly with other found anomalies that exceed the threshold into at least one operationally relevant event indicating a detected event in the network.

Claim 1 of the instant application is directed to a technique that uses connection pattern information and existence of other anomalies to detect unauthorized access, as stated above. In contrast, claim 1 of the co-pending application '376 is directed to finding anomalies by producing a moving average of a parameter associated with network packet flows. In contrast, claim 1 of the instant application uses connection pattern information not moving averages of parameters of network packet flows. These claims are directed to patentably distinct subject matter and therefore neither of the sets of claims are anticipated by or obvious over the other.

The examiner rejected Claims 1-33 on the ground of non-statutory obviousness-type double patenting as being unpatentable over amended claims 1-36 of co-pending application 10/701,404. The examiner stated:

Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant case, all elements of claims 1-33 correspond to the claims of 1-36 of the copending application, except in the instant claims the elements "retrieving connection pairs from a connection table for a host that is attempting to gain access to another host" referred in the copending claims as "adding host-pair connection records to a connection table each time a host accesses another host" and "wherein the connection table is a current time-slice connection table and host pair records are added to the current time slice connection table". Copending claims recite, "determining from the connection table statistics about TCP reset (RST) packets and ICMP port-unreachable packets to

**detect a spike in the number of RST packets and ICMP port-unreachable packets relative to the profile to increase the severity of a port scan event" which encompasses the instant application claims "determining whether the connection requests use the transport control protocol (TCP)" and "determining if other anomalies in the connection patterns of each host exist to establish an event severity level indicating a likelihood that the host attempting to access another host is attempting an unauthorized access". Thus copending application claims anticipates the instant claims.**

Claim 1 of the instant application (as currently amended) is reproduced above.

Claim 1 of the '404 application is:

1. A method of detecting scanning attacks, comprises:  
adding host-pair connection records to a connection table each time a host accesses another host;  
at the end of a short update period, accessing the connection table to determine new host pairs;  
determining the number of new host pairs added to the table over the short update period; and  
if a host has made more than a first threshold number "C1" host pairs, and the number of host pairs is smaller than the threshold number by a first factor value "C2", then  
indicating that the new host is a scanner.

Claim 1 of the instant application is directed to a technique that uses connection pattern information and existence of other anomalies to detect unauthorized access, as stated above. In contrast, claim 1 of the co-pending application '404 is directed method of detecting scanning attacks by determining the number of new host pairs added to the connection table over a short update period and comparing the number to a threshold number of new hosts to see if it is smaller than the threshold number by a value, to indicate that the new host is a scanner. These claims are directed to patentably distinct subject matter and therefore neither of the sets of claims are anticipated by or obvious over the other.

35 U.S.C § 101

The examiner rejected Claims 1-33 under 35 U.S.C. 101 allegedly because the claimed invention is directed to non-statutory subject matter. The examiner stated:

**Claim(s) 31 - 33 are not limited to tangible embodiments as they recite configured for "determining", "receiving" and "sending" functions, which do not define any structural and functional interrelationships between the method, program or instructions and other claimed aspects of the invention, which permits the program's functionality to be realized.**

**The rejection of the base claim is necessarily incorporated into the dependent claims.**

Claim 1 was amended to call for a "computer implemented method." Claim 1 is now directed to statutory subject matter.

Claim 12 was amended to call for a computer program product embodied on a computer readable medium for detecting unauthorized access in a computer network comprising instructions for causing a computing device to." Claim 11 was and still is directed to statutory subject matter. Claim 23, as originally filed, is directed to an apparatus including a processing device and a memory and is clearly directed to statutory subject matter.

### 35 U.S.C. § 102

The examiner rejected Claims 1-33 under 35 U.S.C. 102(e) as being anticipated by Gupta et al. (US Patent 7,234,168). The examiner stated:

**As per Claims 1, 12 and 23, Gupta teaches "retrieving connection pairs from a connection table for a host that is attempting to gain access to another host; determining whether that one host attempting to gain access has accessed the other host accessed previously; and if that one host has not accessed the other host previously, determining if other anomalies in the connection patterns of each host exist to establish an event severity level indicating a likelihood that the host attempting to access another host is attempting an unauthorized access" (Column 6 lines 3 - 42 and Column 7 lines 10-60).**

Claim 1 includes the features of: "... retrieving connection pairs from a connection table for a host that is attempting to gain access to another host ... and if that one host has not accessed the other host previously, determining if other anomalies in the connection patterns of each host exist to establish an event severity level indicating a likelihood that the host attempting to access another host is attempting an unauthorized access.

Gupta neither describes nor suggests at least the foregoing features of claim 1. The examiner argues that: "Gupta teaches "retrieving connection pairs from a connection table for a host that is

attempting to gain access to another host.”; The examiner however does not give any specific cite to this or to any of the other features of claim 1, but merely gives a cite at the end of the argument to (Column 6 lines 3 - 42 and Column 7 lines 10-60). Presumably, therefore, the examiner finds all of the features of claim 1 residing in that portion of Gupta. Applicant disagrees.

At that passage, Gupta neither describes nor suggests “retrieving connection pairs from a connection table for a host that is attempting to gain access to another host ... .” At Column 6 lines 3 - 42 Gupta discusses anomaly detection and signature analysis. Signature analysis involves finding known patterns in packets,<sup>1</sup> whereas anomaly analysis according to Gupta involves a characterization of the normal behavior of the system.<sup>2</sup> While claim 1 includes features of anomaly detection, claim 1 also requires the feature of retrieving connection pairs. The combination of anomaly detection with using connection patterns of hosts to determine whether “one host has not accessed the other host previously” is neither described nor suggested by Gupta.

The examiner also argues that Gupta teaches: “determining whether that one host attempting to gain access has accessed the other host accessed previously; Gupta mentions unauthorized access and access to hosts. However, Gupta does not mention determining whether one host has attempted to access the other host previously and to use this determination to ascertain whether other anomalies exist in connection patterns to warrant raising the severity of an event.

Accordingly, claim 1 and claims 12 and 23 which include analogous features as claim 1 are neither described nor suggested by Gupta.

As for Claims 2, 13 and 24, at least because Gupta neither describes nor suggests connection patterns of the hosts, and therefore Gupta cannot suggest: “determining other anomalies includes determining whether previous connection patterns of the hosts indicate that the hosts are in roles that are not normal for the hosts.” Indeed, neither at the cited passage (Column 7 lines 29-45) nor elsewhere does Gupta suggest roles, much less using roles of hosts in conjunction with connection patterns to determine other anomalies.

---

<sup>1</sup> Gupta see generally discussion starting at col. 11 line 57.

<sup>2</sup> Id. Col. 6, lines 37-38



Similarly, Claims 3, 14, and 25; Claims 4, 15, and 26; Claims 6, 17, and 28; Claims 7, 18, and 29; and Claims 11, 22, and 33 all of which either directly or indirectly rely on the connection table and/or connection patterns thus further distinguish over Gupta, because as set forth above Gupta does not suggest a connection table or processing based on connection patterns in detection of anomalies.

Claims 9, 20 and 31, which requires roles further distinguishes over Gupta, because as set forth above Gupta does not suggest using roles in detection of anomalies.

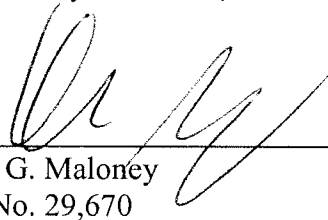
Claims 5, 16 and 27; Claims 8, 19 and 30; and Claims 10, 21 and 32 are allowable at least for the reasons discussed in their respective base claims.

Applicant has enclosed an Information Disclosure Statement. Applicant contends that the claims are allowable over the these references.

Please charge the Petition for Extension of Time fee of **\$60** and please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 12/21/07

  
\_\_\_\_\_  
Denis G. Maloney  
Reg. No. 29,670

Fish & Richardson P.C.  
225 Franklin Street  
Boston, MA 02110  
Telephone: (617) 542-5070  
Facsimile: (617) 542-8906